CLAIMS:

1. Device for running copy-protected software comprising encrypted graphics data (7) and encryption data (8, 11, 12) stored on an information carrier (6), comprising:
- a drive (1) for reading said encrypted graphics data (7) and said encryption data (8, 11, 12),
- means (9) for decrypting said encrypted graphics data (7) using said encryption data (8, 11, 12) for obtaining decrypted graphics data (16),
- an application processing unit (4) for running said copy-protected software,
- a graphics processing unit (10) for processing said graphics data (16),
- means for opening a secure communication channel (5) between said drive (1) and said graphics processing unit (10) for transferring said decrypted graphics data (16) and/or said encryption data (8, 11, 12) from said drive (1) to said graphics processing unit (10)..

2. Device as claimed in claim 1, characterized in that said means (9) for decrypting said encrypted graphics data are included in a graphics card containing said graphics processing unit and said secure communication channel (5) is adapted for transferring said encryption data (8, 11, 12).

3. Device as claimed in claim 1, characterized in that said means (9) for decrypting said encrypted graphics data are included in said drive and said secure communication channel (5) is adapted for transferring said decrypted graphics data (16).

4. Device as claimed in claim 1, characterized in that said encryption data (8, 11, 12) contain key locker data (11) and hidden code data (12) and in that means (13) for unlocking said key locker data (11) by said hidden code data (12) are provided in said drive for obtaining encryption key data (8) for decrypting said encrypted graphics data (7).

5. Device as claimed in claim 1, characterized in that it comprises a game console.

6. Method for running copy-protected software, wherein said copy-protected software is stored on an information carrier (6) and said copy-protected software contains encrypted graphics data (7) and encryption data (8, 11, 12), comprising the steps of:
- reading said graphics data (7) from said information carrier (6),
- reading said encryption data (8, 11, 12) from said information carrier (6),
- decrypting said encrypted graphics data (7) using said encryption data (8, 11, 12) for obtaining decrypted graphics data (16),
- transferring said decrypted graphics data (16) and/or said encryption data (8, 11, 12) via a secure communication channel (5) from said drive (1) to a graphics processing unit (GPU) (10),
- processing said decrypted graphics data (16) by a graphics processing unit (10), and
- processing said copy-protected software by an application processing unit (4).

7. Method as claimed in claim 6, characterized by the steps of
decrypting said encrypted graphics data (7) using said encryption data (8, 11, 12), and
transferring decrypted graphics data (16) to a graphics processing unit (3) via a secure communication channel (5).

8. Method as claimed in claim 6, characterized by the steps of
transferring encryption data (8, 11, 12) via a secure communication channel (5) to a graphics processing unit (3),
transferring said encrypted graphics data (7) to said graphics processing unit (3), and
decrypting said encrypted graphics data (7) using said encryption data (8).

9. Method as claimed in claim 6, characterized in that said encryption data (8, 11, 12) contain key locker data (11) and hidden code data (12) and in that the step of reading out said encryption data comprises the steps of
reading hidden code data (12) from said optical information carrier (6),
reading key locker data (11) from said optical information carrier (6), and
unlocking said key locker data (11) using said hidden code data (12) for obtaining an encryption key (8) for decrypting said encrypted graphics data (7).